UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,491	09/30/2003	Jeyhan Karaoguz	14822US02	6014

23446 7590 08/26/2009

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
RYAN, PATRICK A	

ART UNIT	PAPER NUMBER
2427	

MAIL DATE	DELIVERY MODE
08/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/675,491
Filing Date: September 30, 2003
Appellant(s): KARAOGUZ ET AL.

Mr. Joseph M. Butscher
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed May 27, 2009 appealing from the Office action mailed March 9, 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,182,094	Humpleman et al.	1-2001
2002/0004832	Yoon et al.	1-2002
2003/0177249	Takanashi	9-2003
6,774,926	Ellis et al.	8-2004
6,934,858	Woodhill	8-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims as presented in Final Office Action mailed March 9, 2009 ("Final Office Action"):

Claims 1-12, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis et al., United States Patent (6,774,926 B1), hereinafter "Ellis", in view of Takanashi et al., United States Patent Application Publication (2003/0177249 A1), hereinafter "Takanashi".

In regards to Claim 1, Ellis teaches a method for establishing a communication pathway for subsequent media exchanges between a television display in a first home and storage that contains media in a second home (As shown Figs. 1 and 7, multiple

User Equipment, such as Contributor 102 and Viewer 104, interact over Communications Network 106. Furthermore, Contributor 102 can have storage equipment that viewers on the network, such as Viewer 104, can access and use to retrieve programs, as described in Col. 10 Lines 17-33. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In addition, each of Contributor 102 and Viewer 104 can be required to enter a password, Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach securely transferring authorization and addressing information between a television in a first home and a storage in a second home or requesting confirmation of the security information.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037]. The User ID and password allow the authorization and addressing information to be securely transferred

to the user. In addition, IP Assignment System 125 forwards the IP address, leasing time, and renewal window data to the client in a DHCP reply packet ("Storing Affirmative Confirmation"), as Takanashi discloses in Paragraph [0022].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the method of providing a communications channel between users on a network using a central server, which is accessed by password, as taught by Ellis; with the method of assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet, as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).

In regards to Claim 2, the combination of Ellis and Takanashi teach the method according to Claim 1, comprising associated with the subsequent media exchanges, verifying that the affirmative confirmation has been stored (DHCP reply packet of Takanashi includes a leasing time and renewal window, as described in Paragraph [0022]. Based on the renewal window, the client system must return a renewal packet to Access System 145 in order to continue affirmative confirmation of the assigned IP address, as Takanashi teaches in Paragraphs [0023]; with further reference to Figs. 6 and 7, as described in Paragraph [0034-0037]).

In regards to Claim 3, the combination of Ellis and Takanashi teach the method according to Claim 2, comprising receiving one or both of the address correlation

information associated with the television display in the first home and/or the address correlation information associated with the storage in the second home via at one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

In regards to Claim 4, the combination of Ellis and Takanashi teach the method according to Claim 1, wherein one or both of the address correlation information associated with the television display in the first home and the address correlation information associated with the storage in the second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification, and/or a key (Takanashi teaches address correlation information in the form of IP address assignments, as described in Paragraphs [0022-0023, and 0034]; with further reference to Fig. 6).

In regards to Claim 5, the combination of Ellis and Takanashi teach the method according to Claim 1, further comprising limiting a period for which one or both of the address correlation information associated with the television display in the first home and/or the address correlation information associated with the storage in the second home is valid (Takanashi teaches the use of leasing and renewal time, which limits the

window of time in which an IP address assigned to a client is valid, as described in Paragraphs [0032-0033, and 0036-0037]; with further reference to Figs. 5A, 5B, and 7).

In regards to Claim 6, Ellis teaches a method for establishing a communication pathway for subsequent media exchange between a first media component in a first home and a second media component in a second home (As shown Figs. 1 and 7, multiple User Equipment, such as Contributor 102 and Viewer 104, interact over Communications Network 106. Furthermore, Contributor 102 can have storage equipment that viewers on the network, such as Viewer 104, can access and use to retrieve programs, as described in Col. 10 Lines 17-33. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In addition, each of Contributor 102 and Viewer 104 can be required to enter a password, Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach transferring authorization and addressing information between a media component in a first home and a media component in a second home or requesting confirmation of the information.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is

compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the method of providing a communications channel between users on a network using a central server, which is accessed by password, as taught by Ellis; with the method of assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet, as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).

In regards to Claim 7, the combination of Ellis and Takanashi teach the method according to Claim 6, comprising storing the confirmation (IP Assignment System 125 forwards the IP address, leasing time, and renewal window data to the client in a DHCP reply packet, as Takanashi discloses in Paragraph [0022]).

In regards to Claim 8, the combination of Ellis and Takanashi teach the method according to Claim 7, comprising associated with the subsequent media exchange, verifying that the confirmation has been stored (DHCP reply packet of Takanashi includes a leasing time and renewal window, as described in Paragraph [0022]. Based

on the renewal window, the client system must return a renewal packet to Access System 145 in order to continue affirmative confirmation of the assigned IP address, as Takanashi teaches in Paragraphs [0023]; with further reference to Figs. 6 and 7, as described in Paragraph [0034-0037]).

In regards to Claim 9, the combination of Ellis and Takanashi teach the method according to Claim 6, comprising receiving one or more of the address correlation information in the first home, the address correlation information in the second home and/or the routing address via one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

In regards to Claim 10, the combination of Ellis and Takanashi teach the method according to Claim 6, wherein one or both of the address correlation information in the first home and/or the address correlation information in the second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key (Takanashi teaches address correlation information in the form of IP address assignments, as described in Paragraphs [0022-0023, and 0034]; with further reference to Fig. 6).

In regards to Claim 11, the combination of Ellis and Takanashi teach the method according to Claim 6, further comprising limiting a period for which one or both of the address correlation information in the first home and the address correlation information in the second home is valid (Takanashi teaches the use of leasing and renewal time, which limits the window of time in which an IP address assigned to a client is valid, as described in Paragraphs [0032-0033, and 0036-0037]; with further reference to Figs. 5A, 5B, and 7).

In regards to Claim 12, Ells teaches a system that supports media exchange between a first home and a second home, system comprising: a television display in the first home and storage that contains media in a second home (Personal Television Program System 30 of Fig. 1; with further reference to Fig. 7 showing a Contributor at User Equipment 102 and a Viewer at User Equipment 104, as described in Col. 7 Line 27-Col. 8 Line 16. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In addition, each of Contributor 102 and Viewer 104 can be required to enter a password, Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach transferring authorization and addressing information between a television display in a first home and a storage in a second home or requesting confirmation of the information by way of a secure server.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037]. In addition, Access Control Server 140, shown in Fig. 1 and further detailed in Fig. 4, is used to validate the client's User ID and password, and control a client's access to Network 110, as described in Paragraph [0031].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the system for providing a communications channel between users on a network using a central server, which is accessed by password, as taught by Ellis; with the system for assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet, as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).
In regards to Claim 14, the combination of Ellis and Takanashi teach the system according to Claim 12, wherein the one or both of the first routing address and/or the

second routing address is communicated via at one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

In regards to Claim 15, the combination of Ellis and Takanashi teach the system according to Claim 12, wherein the server authenticates an initial access of one or both of the television display having an associated first routing address and/or the storage having an associated second routing address (Takanashi teaches Access System 145 of Access Control Server 140 that verifies a clients User ID and password before assigning the client an IP address, as described in Paragraph [0036]).

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ellis and Takanashi as applied to Claim 15 above, and further in view of Humpleman et al., United States Patent (6,182,094 B1).

In regards to Claim 13, the combination of Ellis and Takanashi teach the system according to Claim 12. In addition, Takanashi teaches that DHCP server 120 assigns P address to clients on the network and can reallocate the IP address if the IP assignment is cancelled (as discussed in Paragraph [0007]). Takanashi's disclosure suggests, but

does not explicitly teach that the server comprises a memory that stores one or both of the first routing address and/or the second routing address.

In a similar field of invention, Humpleman teaches a method and system using a DHCP server (106/306) that acts as a configurations manager for Home Network 100, with reference to Figs. 1 and 4A. In addition, Humpleman teaches that DHCP Server stores the generated IP addresses and logical name pair within a device list, as described in Col. 11 Lines 35-55 and Col. 12 Lines 12-21.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of providing a secure communications channel in a media exchange network, as taught by the combination of Ellis and Takanashi to include a DHCP server that stores the IP addresses of clients on the network, as taught by Humpleman, in order to have a centrally stored record of all devices on the network and a record of IP addresses that have been assigned and that are available.

Claims 16-18, and 20-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of Yoon et al., United States Patent Application Publication (2002/0004832 A1), hereinafter “Yoon”.

In regards to Claim 16, Ellis teaches a system for communicating information (Personal Television Program System 30 of Fig. 1; with further reference to Fig. 7), the system comprising: a first device (Data Storage Facility 52 of Fig. 1 that hosts an interface for allowing a contributor of media and a viewer of media to enter a password

in order to gain access to the communications network, as described in Col. 11 Line 53 - Col. 12 Line 16. In addition, the operations of Data Storage Facility 52 can be performed by one or more servers, such as Servers 112, 116, or 118 or Fig. 7, as described in Col. 4 Lines 59-67), a second device (Viewer at User Equipment 104 of Fig. 7, as described in Col. 7 Line 27-Col. 8 Line 16), and a third device (Contributor at User Equipment 102). In addition, Ellis teaches that Contributor at User Equipment 102 transfers media to the Viewer at User Equipment 104, as described in Col. 3 Line 55 – Col. 4 Line 5.

Ellis does not teach a processor used to issue access information to a second and third device by way of a first device or that the processor authenticates access information between the second and third devices.

In a similar field of invention, Yoon teaches a system and method for establishing a communications channel between a Local Computer 30 and an Internet Server 60 (Abstract, with further reference to Figs. 1 and 4). Yoon also teaches the communicating and assigning access information in the form of a Temporary ID and Password that is assigned based on the confirmation of a requester's IP address. In addition, Yoon teaches a processor, Connection Authentification Server 50, which communicates access information between the Local Computer 30 and the Internet Server 60, as described in Paragraphs [0030-0032]. The Connection Authentification Server 50 transfers access information to the Local Computer 30 through the process of Steps 100 and 102 ["from first to third device" where the processor resides at the first device]. In addition, the Connection Authentification Server 50 issues this access

information to the Internet Server 60 is Step 104 of Fig. 4 ["first to second device"]. Yoon also teaches that Local Computer 30 request connection authentification in Step 100 before requesting the services of Internet Server 60 ["authenticates the access information"] (as described in Paragraphs [0038-0039], with reference to Fig. 4; with further reference to Step 314 of Fig. 6, as described in Paragraph [0060-0061]).

Both Ellis and Yoon teach communication systems in which a secure communications pathway is established between devices on a network. In addition, both Ellis and Yoon utilize a server to authenticate the devices that request access to the network. Ellis teaches requiring each user on the network to enter a password in order to gain access and transfer media by way of a central server (using Data Storage Facility 52). Yoon teaches authenticating a user's IP address and then issuing a Temporary IP and Password so that the user can access the network (using Connection Authentification Server 50). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for providing a communications channel between users on a network, which is accessed by password, as taught by Ellis, to include the Connection Authentification Server taught by Yoon in order to enhance the security of the system (as Yoon describers in Paragraph [0013]). In regards to Claim 17, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor communicates the access information from the at least the second device to the third device (Yoon teaches the transmission of Connection Admission Signal 108 from Internet Server 60 to Local Computer 30, as shown in Fig. 4 and described in Paragraphs [0038-0039]).

In regards to Claim 18, the combination of Ellis and Yoon teach the system according to Claim 17, wherein the at least one processor communicates the access information from the at least the second device to the third device via one or both of an in-band channel and/or an out-of-band channel (Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

In regards to Claim 20, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the first device is a media exchange server (Ellis teaches Data Storage Facility 52 of Fig. 1 as described in Col. 4 Lines 42-67; with further reference to Fig. 7).

In regards to Claim 21, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least the second device and the third device is one or more of a media processing system, a personal computer executing media exchange software, and a media peripheral (Ellis teaches User Equipment 102 and 104, which can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56).

In regards to Claim 22, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor permits the third device to communicate with the at least the second device, if the access information is authenticated by the first device (Authentification Server 50 determines the authenticity

of the IP address "N" received from Local Computer 30, as shown in Step 306 of Fig. 6 and described in Paragraphs [0052-0055]. If Local Computer 30 is authenticated, a Temporary ID and Password are generated at Step 314, which are used to open the communications channel as show in Step 110 of Fig. 4, as described in Paragraph [0039]).

In regards to Claim 23, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor one or both of denies and/or restricts the transfer of the at least one of media, data, and, service between the at least the second device, if the access information is not authenticated by the first device (Authentification Server 50 determines the authenticity of the IP address "N" received from Local Computer 30, as shown in Step 306 of Fig. 6 and described in Paragraphs [0052-0055]. If Local Computer 30 is not authenticated then Step 318 is executed where a refusal signal is transmitted, which denies Local Computer 30 access to the network, as described in Paragraph [0055]).

In regards to Claim 24, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the access information is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key (Yoon teaches a Temporary ID and Password that is assigned based on the confirmation of a requester's device identification in the form of an IP address, as described in Paragraph [0038]).

In regards to Claim 25, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor limits a period for which the access information is valid (Yoon teaches Authentification Server 50 can assign an Authentification Time "T" to the Temporary ID and Password, as disclosed in Paragraph [0058]; with further reference to Step 408 of Fig. 7, as described in Paragraph [0068]).
In regards to Claim 26, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor is one or more of a computer processor, a media peripheral processor, a media exchange system processor, a media exchange server processor and/or a media processing system processor (Ellis teaches a media exchange system processor shown as Data Storage Facility 52 of Fig. 1 and described in Col. 4 Lines 42-67; with further reference to Fig. 7).

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ellis and Yoon as applied to Claim 17 above, and further in view of Woodhill, United States Patent (6,934,858 B2).

In regards to Claim 19, the combination of Ellis and Yoon teach the system according to Claim 17, but the combination does not teach system comprising a telephone device that is utilized to inform a user of the third device of the access information.

In a similar field of invention, Woodhill teaches a method and system for authenticating and authorizing a user wishing to participate in an electronic transaction on a communications network (Abstract, with further reference to Fig. 1). Woodhill teaches the use of Public Switched Telephone Network 44 and Telephone 46 in order to provide a user with confirmation information. This confirmation information is used to authenticate the user by way of Authentication/Authorization Service 38 for access to Target Site 30 (as shown in Fig. 1 and described in Col. 8 Lines 12 – Col. 9 Line 5). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for establishing a communications channel between authorized devices on a network, as taught by the combination of Ellis and Yoon, to include a telephone device to inform a user of access information, as taught by Woodhill, in order to provide a real-time and secure means of authenticating a user (as Woodhill describes Col. 5 Line 24 - Col. 6 Line 23; with further reference to Table II in Col. 5).

(10) Response to Argument

The Examiner respectfully disagrees that the rejection should be reversed. Only those arguments having been raised are being considered and addressed in the Examiner's Answer. Any further arguments regarding other elements or limitations not specifically argued or any other reasoning regarding deficiencies in a prima facie case of obviousness that the Appellant could have made are considered by the Examiner as having been conceded by the Appellant for the basis of the decision of this appeal. They are not being addressed by the Examiner for the Board's consideration. Should the

panel find that the Examiner's position/arguments or any aspect of the rejection is not sufficiently clear or a particular issue is of need of further explanation, it is respectfully requested that the case be remanded to the Examiner for further explanation prior to the rendering of a decision.[1]

Response to Appeal Brief Section I: The Proposed Combination Of References Does Not Describe, Teach Or Suggest "Requesting Affirmative Confirmation Using Said Received Address Correlation Information Associated With One Or Both Of The Television Display And/Or The Storage" or "Storing a Request for Confirmation"

The Examiner first submits the following regarding the scope of the Claim 1 step: "requesting affirmative confirmation using said received address correlation information…"

Page 4 Lines 13-17 of the Specification state: "[t]he address correlation information associated with the television display in the first home and the address correlation information associated with the storage in the second home may be a digital certificate, a one-time digital certificate, a one-time code, a device identification, a key or a combination thereof". Additionally, Page 15 Lines 9-12 state: "a one time digital certificate may contain information such as a device ID, a public key, an IP address, a one-time code or a pin number, and other information that may be somewhat related to services that may be provide".

[1] See 37 CFR 41.50(a)(1) and MPEP 1211.

Page 15 Lines 1-4 state: "[i]n step 205 [of Fig. 2A], the media exchange server may attempt to confirm the authenticity of the digital certificate information provided by the second device. In this regard, confirmation may be achieved by utilizing the device ID of the first device". Additionally, "[i]n step 206, if confirmed then, in step 207, the media exchange server may authorize the second device to push media to the first device over the media exchange network" (Page 15 Lines 4-6). In view of Step 206 "Confirmed?" of Fig. 2A, the Examiner construes an "affirmative" confirmation to be one in which a decision of "Yes" (or generally, an outcome of truth or validity) is found in the confirmation step, which results in the authorization of the device requesting access. The Examiner also notes that a similar confirmation step is performed using a "one-time code" in Step 215 of Fig. 2B as described on Page 18 Lines 14-24.

Page 14 Lines 17-21 state: "a first device at a first location may request a one-time digital certificate, which may be associated with a device identification (ID) of the first device. In this regard, the one-time digital certificate may be requested from a media exchange server and may be utilized for communication or media exchange on a media exchange network."

Claim 1 recites the steps of "securely receiving…", "requesting…", and "storing…", however the claim does not specify that these steps are to be preformed by a particular element of the media exchange system. For example, as claimed, the act of "requesting" could be associated with elements of "the first home" or "the second home"; or, in view of the Specification, a third party such as a media exchange server. Additionally, the limitation "requesting affirmative confirmation" does not clearly

establish what is being confirmed. In view of the above cited passages of the Specification, the Examiner has construed that the act of "requesting affirmative confirmation" is a request for validation of the authenticity of the address correlation information (i.e. digital certificate, one time code, device identification), where this request originates from the device attempting to access the system.

The Examiner relies upon Ellis to teach a method for establishing a communication pathway for subsequent media exchanges between a television display in a first home and storage that contains media in a second home. For example, in Figure 7 Ellis demonstrates User Equipment connected to Communications Network 106, such as Contributor 102 and Viewer 104, where the Contributor can have storage that Viewers on the network can access and use to retrieve programs (as Ellis describes in Col. 10 Lines 17-33). The Examiner has additionally pointed out that Ellis teaches that each of the Contributor 102 and Viewers 104 can be required to enter a password in order to modify or gain access to stored content (as Ellis demonstrates with Options 200 and 213 of Fig. 14, and as described in Col. 11 Line 53—Col. 12 Line 16). Therefore, Viewer 104 gains access to the storage of Contributor 102 when the correct password is entered by the Viewer. The Examiner notes that the citation of Ellis's password is indented to demonstrate a general security feature for limiting access to media within a known media exchange system.

The Takanashi reference is relied upon to teach the Claim 1 limitations of securely receiving address correlation information, requesting affirmative confirmation using the address correlation information, and storing the affirmative confirmation. In

particular, Takanashi uses Dynamic Host Configuration Protocol (DHCP) to assign Internet Protocol (IP) addresses to client devices attempting to access a network, where a random leasing time and/or renewal time is assigned to each IP address, as demonstrated in the method of Figure 6 and described in Paragraphs [0009, 0034-0035]. Takanashi additionally discuses requiring a user's ID and password to enable the client to login to the network (i.e. gain access) once the information provided is judged to be valid (Paragraphs [0009, 0022-0024]).

Appellant presents (Appeal Brief received May 27, 2009 ("Brief") Section I Subsection A, starting on Page 7) that Takanashi does not teach the limitation "requesting affirmative confirmation using said received address correlation information" because "[a] request for an IP address is not, however, a request for confirmation, in general, nor a request for confirmation using received address correlation information associated with one or both of a television display and/or a storage, in particular" (Brief Page 8 and Takanashi [0009, 0028, 0034-0036]). Appellant further presents that "an IP address request may be made without requesting confirmation" (Brief Page 8) and that "[t]he mere act of 'logging onto' a network using an IP address, a user ID and/or password is by no means a 'request'" (Brief Page 9).

The Examiner first notes that Appellant does not provide evidence by way of the Specification, cited references, or ordinary knowledge that "an IP address request may be made without requesting confirmation." As presented above, the Examiner has construed, in view of the Specification, that the act of "requesting affirmative confirmation" is a request for validation of the authenticity of the address correlation

information (i.e. digital certificate, one time code, device identification), where this request originates from the device attempting to access the system. The Examiner has not simply associated Appellant's claimed "requesting affirmative confirmation" with the request for an IP address or an act of logging onto a network, but more broadly an act of validating a client attempting to access a network.

As presented in Final Office Action Page 8, the Examiner has addressed the "address correlation information" aspect of Claim 1 with Takanashi's assignment of IP addresses (as Takanashi discusses in Paragraphs [0034-0035] and Fig. 6). It is the Examiner's position that Appellant's Specification (Page 4 Lines 13-17, Page 15 Lines 9-12) demonstrates that an IP address constitutes "address correlation information", as presented above. Additionally, as Takanashi discusses in Paragraph [0034], "IP assignment system 125 receives (610) a request for an IP address in the form of a DHCP broadcast from a client." The Examiner submits that the "request" at Step 610 of Takanashi has not been associated with Appellant's claimed "requesting". To clarify, according to Network Working Group Request for Comments 2131 "Dynamic Host Configuration Protocol" ("RFC 2131") [2], Takanashi's Step 610 "DHCP broadcast from a client" is a "DHCPDISCOVERY message", as shown in the Timeline in Figure 3 on Page 14. More specifically, the DHCPDICOVERY and DHCPOFFER messages function to "correlate" the addresses of the client and the server so that communication can be established between them (RFC 2131 Page 15 in section 3.1 subsection 3).

[2] "Internet Engineering Task Force", Request for Comments 2131, Dynamic Host Configuration Protocol (DHCP) Mar. 1997, pp. 1-43. Accessed from <http://www.ietf.org/rfc/rfc2131.txt> on August 14, 2009

The Examiner has addressed the act of "requesting affirmative confirmation using said received address correlation information" with Takanshi's teachings of a client device logging onto Network 110, which requires a valid IP address, and a User ID and password (Office Action Page 5; Takanashi [0022-0024]). The Examiner emphasizes that this process requires a valid IP address. The Examiner submits that the validity of the address is a function of the availability of the IP address and assigned leasing/renewal time (Steps 630-640 of Takanshi, as described in Paragraph [0034]). Additionally, the Examiner submits that this portion of the DHCP process involves a request to the DHCP server. In particular, according to RFC 2131, a DHCPREQUEST message is transmitted from the client to the selected server, where "[t]he server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client" (RFC 2131 Page 15 section 3.1 subsection 4). Additionally, "[i]f the selected server is unable to satisfy the DHCPREQUEST message (e.g., the requested network address has been allocated), the server should respond with a DHCPNAK message" (RFC 2131 Page 15 section 3.1 subsection 4). It is the Examiners position that the server's transmission of a DHCPACK message represents an "affirmative confirmation" because this process establishes a valid IP address for the client and additionally notes that this is the function of the DHCP reply packet transmitted during the login process of Takanashi (as described in Paragraph [0022]).

Appellant presents (Brief Section I Subsection B, starting on Page 10) that Takanashi does not teach the limitation "storing said affirmative confirmation" because a "stored user ID and password are not the same as a stored affirmative confirmation" (Brief Page 10 and Takanashi [0031]).

The Examiner has presented that Takanashi demonstrates the storage of affirmative confirmation by way of a DHCP reply packet containing the IP address, leasing time, and renewal window data (Final Office Action Page 8 and Takanashi Paragraph [0022-0023]). As the Examiner has noted above, affirmative confirmation is sent to the client device by way of the DHCP reply pack, which contains a lease time. The Examiner submits that this lease time is inherently stored during the DHCP process because the client must know the time frame in which to transmit a renewal request and the server must know if this request was received within the renewal window. For example, RFC 2131 explicitly demonstrates that the client device must store this information in order to determine when a renewal packet is to be transmitted (RFC 2131 Section 4.4.1 Page 37). Additionally, "[t]he server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client" (RFC 2131 Page 15 section 3.1 subsection 4). The Examiner notes that neither the claims nor the specification of the instant application particularly define the scope of the storing limitation and therefore this limitation can be reasonably associated with the client, the server or both.

Therefore, the Examiner submits that the combination of Ellis and Takanshi does in fact teach the Claim 1 limitation "requesting affirmative confirmation using said received address correlation information" and “storing said affirmative confirmation”. Appellant does not present additional substantive arguments in Brief Section I regarding the limitations of Claims 2-12 and 14-15, therefore the Examiner submits that the reasoning presented above sufficiently addresses these issues.

Response to Appeal Brief Section II: The Proposed Combination Of Ellis And Takanashi Does Not Render Claims 2 And 8 Unpatentable For An Additional Reason.

Appellant presents (Brief Section II on Page 12) that the combination of Ellis and Takanashi does not teach the Claim 2 limitation of “associated with the subsequent media exchanges, verifying that said affirmative confirmation has been stored” because in addition to Takanashi’s deficiencies in addressing Claim 1, Takanashi does not discloses verifying the storage of affirmative confirmation.

As presented above, it is the Examiner’s position that Takanashi teaches the storage of affirmative confirmation by way of a DHCP reply packet including an IP address, leasing time, and renewal window. Additionally, as the Examiner has presented in Final Office Action Page 9, Takanashi discloses the use of a “renewal window” in which the client device must transmit a renewal packet in order to extend the leasing time and access to the network (Takanashi Paragraph [0023]). In particular, Figure 7 of Takanashi demonstrates the process of “verifying” the renewal packet to

determine if the client device should or should not continue to have access to the network, as described in Paragraphs [0036-0037].

Therefore the Examiner submits that the combination of Ellis and Takanashi do in fact teach the Claim 2 limitation of "associated with the subsequent media exchanges, verifying that said affirmative confirmation has been stored". Appellant does not present additional substantive arguments in Brief Section II regarding the limitations of Claim 8, therefore the Examiner submits that the reasoning presented above sufficiently addresses these issues.

Response to Appeal Brief Section III: The Proposed Combination Of Ellis, Takanashi And Humpleman Does Not Render Claim 13 Unpatentable

Appellant does not present additional substantive arguments in Brief Section III regarding the limitations of Claim 13, therefore the Examiner submits that the reasoning presented above sufficiently addresses these issues (with particular reference to Claim 1).

Response to Appeal Brief Section IV: The Proposed Combination Of Ellis And Yoon Does Not Render Claims 16-18 And 20-26 Unpatentable

Appellant presents (Brief Section IV, staring on Page 13) that the combination of Ellis and Yoon does not teach "at least one processor that issues access information from a first device to at least a second device" because the Final Office Action associates the Connection Authentification Server 50 of Yoon with both the "at least one

processor" and the "first device" (Brief Pages 13-14). Appellant additionally presents that Yoon does not teach the limitation "said at least one processor authenticates said access information by said first device when said third device attempts to transfer at least one of media data and service to said at least said second device" because "Yoon states that the local computer 30 requests a connection authentication to the connection authentication server 50 before requesting services to the target internet server 60" (Brief Pages 14-15; Yoon [0038]).

The Examiner submits that neither Claim 16 nor the specification particularly define that the "at least one processor" and the "first device" must be separate entities within the media exchange system. Additionally, the Examiner notes that Claim 16 requires "access information" to be issued from "a first device to at least a second device", but does not state that the "processor" issues access information to the "first device". Therefore, it is the Examiner's position that the processor of Claim 16 can reasonably be interpreted as part of the first device.

In addressing Claim 16, the Examiner has identified Local Computer 30 as the claimed "third device" and Target Internet Server 60 as the claimed "second device" (Final Office Action Pages 16-18; Yoon Figs. 1 and 4). In Yoon's method of Fig. 4, Local Computer 30 is attempting to transfer a request for connection to Internet Server 60 (which the Examiner has associated with the claimed "service"; performed at Step 106 of Fig. 4) and that this attempt commences at the beginning of the process of Fig. 4 (i.e. Step 100). It is the Examiner's position that Local Computer 30's request to Authentification Server 50 is just a step in the process of attempting to transfer a

request for connection to Internet Server 60. The Examiner submits that no particular time frame is established in Claim 16 to provide any particular meaning to the word "when" and that the claim merely requires that the even occurs. Additionally, Applicant's use of the word "comprising" does not preclude the Examiner from using additional structural or functional aspects that are not claimed in addressing the stated claim language. Therefore, the Examiner upholds that Yoon does in fact teach the Claim 16 limitation of "said at least one processor authenticates said access information by said first device when said third device attempts to transfer at least one of media data and service to said at least said second device".

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Patrick A Ryan/
Examiner, Art Unit 2427

Conferees:
(Scott Beliveau, Jason Salce)

/Scott Beliveau/
Supervisory Patent Examiner, Art Unit 2427

/Jason P Salce/
Primary Examiner, Art Unit 2421